IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1. (Currently Amended) An information reproducing apparatus, comprising:

a secure module that stores a first information, wherein the secure module can not be accessed from outside;

a memory that stores a second information, wherein the memory can be accessed from outside;

a falsification checking unit that is loaded on the secure module, wherein the falsification checking unit reads the second information from the memory by direct access, compares the second information with the first information in the secure module, and checks a falsification of the second information based on a result of the comparison; and

a reproducing unit ~~reproducing~~ playing-back the second information when a result of the check by the falsification checking unit is that the second information is not falsified.

2. (Original) The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads all of the second information.

3. (Original) The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads a part of the second information.

4. (Original) The information reproducing apparatus according to claim 1, wherein the falsification checking unit performs the comparison of the first information and the second information using a checksum method.

5. (Original) The information reproducing apparatus according to claim 1, wherein herein the second information is software.

6. (Previously Presented) The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads the second information from the memory on an

irregular basis.

7. (Previously Presented) The information reproducing apparatus according to claim 1, further comprising:

an storing unit that is loaded on the secure module and that updates the second information in the memory using a direct access method.

8. (Previously Presented) The information reproducing apparatus according to claim 7, wherein the storing unit updates the second information on an irregular basis.

9. (Previously Presented) The information reproducing apparatus according to claim 7, wherein the storing unit updates a part of the second information.

10. (Previously Presented) The information reproducing apparatus according to claim 7, wherein the falsification checking unit reads the second information updated by the storing unit.

11. (Previously Presented) The information reproducing apparatus according to claim 7, wherein when the second information is updated, the storing unit changes over the second information which has been updated.

12. (Previously Presented) The information reproducing apparatus according to claim 7, wherein the storing unit stores the second information after encryption using a key that exists in the secure module.

13. (Previously Presented) The information reproducing apparatus according to claim 1, further comprising:

a key managing unit that is loaded on the secure module, wherein the key managing unit holds a key used to encrypt or decode the second information, and the key managing unit outputs the key, if the falsification checking unit does not detect a falsification.

14. (Original) The information reproducing apparatus according to claim 13, wherein the key supplied by the key managing unit is valid only for a predefined period of time.

15. (Previously Presented) The information reproducing apparatus according to claim 13, wherein the key managing unit changes the key each time the key managing unit outputs the key.

16. (Previously Presented) The information reproducing apparatus according to claim 13, wherein when the falsification checking unit detects a falsification, the key managing unit does not output the key.

17. (Original) The information reproducing apparatus according to claim 1, further comprising:

a writing unit that is loaded on the secure module, wherein the writing unit writes a secret information within the secure module into the memory as the second information using the direct access method, wherein

the falsification checking unit checks falsification of the second information based on response information corresponding to the secret information.

18. (Previously Presented) The information reproducing apparatus according to claim 17, wherein the secret information is stored in a controlled memory space, wherein

the controlled memory space is such that a correct information is read out from the memory space at a first time and an incorrect information is read out at a second time.

19. (Original) The information reproducing apparatus according to claim 1, wherein the second information is encrypted MPEG data.

20. (Currently Amended) An information reproducing method comprising:

reading second information stored in a memory, by a secure module storing a first information, wherein the secure module can not be accessed from outside, and the memory can be accessed from outside using a direct access method;

checking falsification by comparing the second information with the first information, and checking a falsification of the second information based on a result of the comparison; and

~~reproducing~~ playing-back the second information when a result of checking falsification is that the second information is not falsified.

21. (Currently Amended) A secure module mounted to an information reproducing apparatus, comprising:

a reading unit that reads a second information from a memory mounted to a information reproducing apparatus by direct access, wherein the memory can be accessed from outside; and~~;~~

a falsification checking unit that compares the second information with a first information stored in the secure module, and checks a falsification of the second information based on a result of the comparison, wherein if the result of the comparison shows that the second information is not falsified the second information is played-back by the information reproducing apparatus.

22. (Original) The secure module according to claim 21, wherein the reading unit reads all of the second information.

23. (Original) The secure module according to claim 21, wherein the reading unit reads a part of the second information.

24. (Original) The secure module according to claim 21, wherein the falsification checking unit performs the comparison of the first information and the second information using a checksum method.

25. (Original) The secure module according to claim 21, wherein the second information is software.

26. (Previously Presented) The secure module according to claim 21, wherein the reading unit reads the second information from the memory on an irregular basis.

27. (Previously Presented) The secure module according to claim 21, further comprising:

a storing unit that stores the second information in the memory using a direct access method.

28. (Previously Presented) The secure module according to claim 27, wherein the storing unit updates the second information on an irregular basis.

29. (Previously Presented) The secure module according to claim 27, wherein the storing unit updates a part of the second information.

30. (Previously Presented) The secure module according to claim 27, wherein the falsification checking unit reads the second information updated by the storing unit.

31. (Previously Presented) The secure module according to claim 27, wherein when the second information is updated, the storing unit changes over the second information which has been updated.

32. (Previously Presented) The secure module according to claim 27, wherein the storing unit stores the second information after encryption using a key that exists in the secure module.

33. (Previously Presented) The secure module according to claim 21, further comprising:

a key managing unit that holds a key used to encrypt or decode the second information, and the key managing unit outputs the key, if the falsification checking unit does not detect a falsification.

34. (Original) The secure module according to claim 33, wherein the key supplied by the key managing unit is valid only for a predefined period of time.

35. (Previously Presented) The secure module according to claim 33, wherein the key managing unit changes the key each time the key managing unit outputs the key.

36. (Previously Presented) The secure module according to claim 33, wherein when the falsification checking unit detects a falsification, the key managing unit does not output the key.

37. (Original) The secure module according to claim 21, further comprising:

a writing unit that writes a secret information within the secure module into the memory as the second information using the direct access method, wherein the falsification checking unit checks falsification of the second information based on response information corresponding to the secret information.

38. (Previously Presented) The secure module according to claim 37, wherein the secret information is stored in a controlled memory space, wherein the controlled memory space is such that a correct information is read out from the memory space at a first time and an incorrect information is read out at a second time.

39. (Original) The secure module according to claim 21, wherein the second information is encrypted MPEG data.

40. (Currently Amended) A recording medium that records a program for causing a secure module mounted to an information reproducing apparatus to execute a process, the process comprising:

reading a second information stored in a memory mounted to the information reproducing apparatus, wherein the secure module stores a first information, and the secure module can not be accessed from outside, and the memory can be accessed from outside using a direct access method; ~~and~~

checking falsification by comparing the second information with the first information, and determining a falsification of the second information based on a result of the comparison; and

playing-back the second information when the result of the comparison is that the second information is not falsified.

41. (Currently Amended) A method of a reproducing verified information, comprising:

~~reproducing~~ playing-back second information that is stored in a memory accessible from outside an information reproducing apparatus using a direct access method, if comparison of the second information with first information stored in a secure module inaccessible from outside, indicates that the second information is not falsified.